

FilesAnywhere

You've always got it.

Security, Availability, Reliability

TOP PRIORITIES AT FILESANYWHERE

Thank you for your interest in FilesAnywhere. Recognizing the importance of data security, we provide multiple layers of security to protect our customers' data. These layers of protection are described below.

We take security very seriously at FilesAnywhere. It is our aim to provide a world-class service, using all security implements required to protect our customers' data from unauthorized access and uninterrupted access.

Our security procedures are introduced for the public on our website at the following link:

http://www.filesanywhere.com/Help/General_Information/Security.htm



TRANSMISSION SECURITY



SSL encrypts data and ensures security of transmissions between the client computer and FilesAnywhere. SSL is optional for each individual user account, however accounts can be marked as requiring SSL for login, by individuals, workgroup owners, and for all accounts in a Private Site.

ACCOUNT ACCESS SECURITY

In the case of Private Sites and Dedicated Servers, rules for account and password complexity and login rules can be controlled by the designated Administrator. This prevents passwords and account names that are too simple. Additionally, automated account "lockout" features protect against unauthorized access attempts. Private Sites and Dedicated Servers have the additional security benefit of customized IP access rules, which can optionally block unauthorized computers from access to web or mapped drive file access interfaces.



SHARED ACCESS CONTROL

Access control to shared resources is implemented in two ways: GroupShares and FileView shares can assign Full Control, Read-Only, or Create/Update access to shared folders, to each individual assigned. Also, with Private Sites and Dedicated Servers, if FTP or WebDAV is enabled, privileges to common folders can be customized at any level (applied using NTFS directory-level security). Also, we offer fixed IP restrictions as an option on any FTP account, WebDAV account, or Private Site, to restrict traffic to a designated list of computer IP's.



DATA CENTER

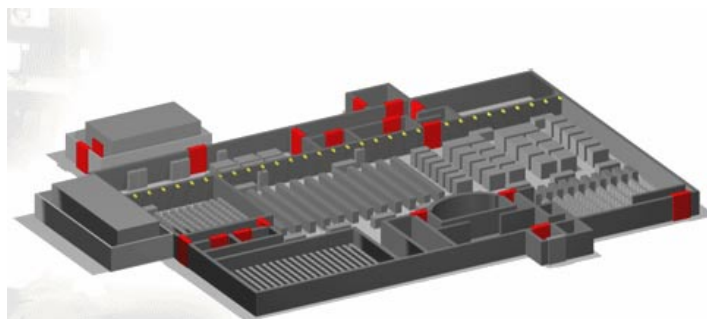
Our main Datacenter is state-of-the-art in both security and design. This facility is one of the only Datacenters in the world rated to withstand an F5 grade tornado.

Extensive, meticulously implemented security measures have been applied at the FilesAnywhere Data Center to ensure the security of our customers' data. We have a dedicated Information Security Team with engineers trained and specialized in data security. They are experts in

security methodology, threat avoidance, detection, and response. We routinely outsource independent security audits from Microsoft and our ISP security team. Our firewalls monitor each packet that enters the data center. We use a combination of Cisco PIX 515e and Watchguard Firebox firewall appliances, in addition to software running on server equipment that monitor security (intrusion detection, virus scanning, system logs, etc.). We have detailed checklists that every server must pass as part of new server deployment to ensure maximum security, and updates are made daily to our threat protection software.

Data Center Specs:

- 60,000 sq. ft. facility
- 35,000 sq. ft. of raised floor
- (21) 26-ton Data Air AC units
- Very Early Smoke Detection Apparatus (VESDA)
- Pre-action dry pipe sprinkler system
- Over 500 smoke detectors in an integrated system
- Simplex security badge entry/exit on all doors to facility
- Multiple TXU electrical grids
- 4800 amps of 480v input power
- 3 main transfer switches
- (6) 500KVA Powerware UPS units with 90 batteries per unit
- Standalone PDUs at each cabinet row
- 1-megawatt generator (2000-gallon tank)
- 1.5-megawatt generator (2200-gallon tank)
- DataTrax monitoring software for all data center infrastructure



The physical security at our data center can be seen at the following infrastructure page:

http://www.filesanywhere.com/Help/General_Information/Data_Center.htm

The timed slideshow at the bottom of the web page will show you first hand the level of physical security employed at our data center. Server access by FilesAnywhere Network Engineering and Information Security teams is controlled via Kerberos and three-factor Authentication (Domain credentials, Kerberos authentication and certificate validation.). Our security tools are monitored 24x7, in real-time. Scheduled vulnerability assessments track deviations from standard baseline.

INTRUSION DETECTION AND PREVENTION

Our IDS management is highly secure, by its nature. Management of IDS systems (and security systems in general) is only available from a certain range of private IP's located on FilesAnywhere's security network segment. Authentication is controlled via Kerberos and RADIUS; SSH access is restricted to Kerberos / public key / authenticated password only. No internet access is allowed. No network routes exist between the internet and our private security management network.



Advanced multi-tiered security protocols that are working together in layers to protect the FilesAnywhere network at all times:

- Cisco Guard DDoS Mitigation
- Tipping Point IPS
- Arbor Peakflow: Notifies NOC analysts of suspicious activities
- ISS: Automated IDS, monitors activity in real-time, for instant response to security breaches
- Spirus: Email gateway that protects hosted mail servers from email attack, spam and viruses
- GFI MailEssentials with Bayesian filtering technology: Protects host servers from email spam

INTERNAL POLICIES

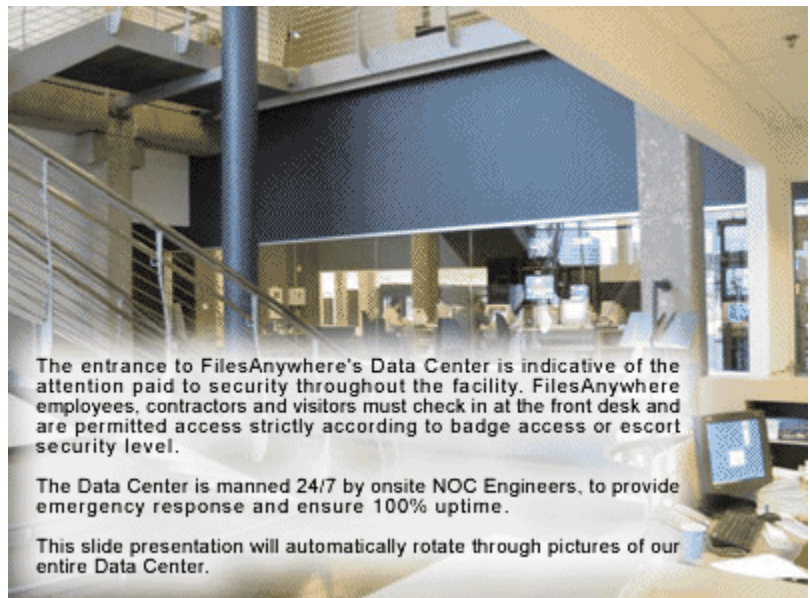
We employ comprehensive internal security policies and procedures, starting at the front door.

Examples of this include:

- Keycard Entry
- Security Guard at Entrance 24-hours
- Monitored surveillance cameras throughout data center
- Microsoft Host Information Security Minimum Requirements
- Linux Systems Information Security Standards.
- Network Device Security Policy
- Network Access Standards
- Security Incident Policy
- Sensitive Data Storage and Access Policy

All employees are required to execute a non-disclosure and non-compete agreement at the time of employment. The non-disclosure agreement defines Company and Customer privacy policies and bounds the employee by contract to those terms for a period of 5 years after termination of employment has occurred.

In addition, we distribute a weekly security newsletter to all staff members of the Information Security team, as well as Quarterly all-hands training and an Annual training session with Law Enforcement participation.



SECURITY OPTIONS ON PRIVATE SITES

There are a number of flexible options and settings that we use to customize your FilesAnywhere Private Site. This allows for tailored security measures and system defaults.

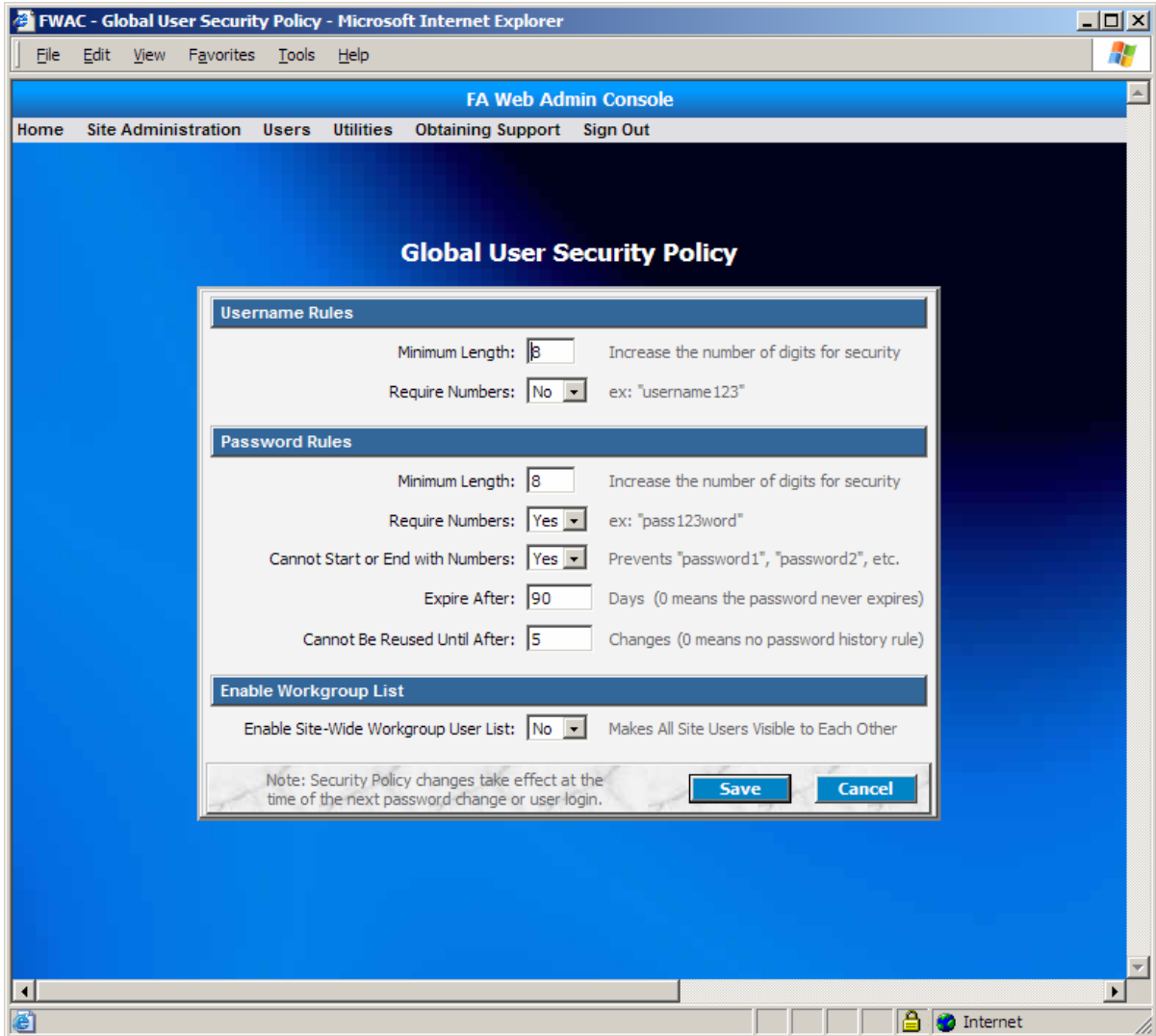
| Security Requirements | Default Setting | Customer Setting |
|---------------------------------------------|-----------------|------------------|
| Minimum Username Length | 4 | |
| Numeric Digit Required in Username | N | |
| Minimum Password Length | 6 | |
| Numeric Digit Required in Password | N | |
| Password Expires After ? Days | Never expires | |
| Non-numeric Boundary in Password | N | |
| Lockout After Maximum Failed Login Attempts | (none) | |
| Lockout After Maximum Logins Per 24 Hours | (none) | |

| System Settings | Default Setting | Customer Setting |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|------------------|
| Display All Site Users in Contacts (all email addresses will be visible to all users) | YES | |
| System-Generated Emails From | support@filesanywhere.com | |
| Feedback Emails Sent To | support@filesanywhere.com | |
| Notification of Max. Failed Attempts Sent To | support@filesanywhere.com | |
| Support Emails Sent To | support@filesanywhere.com | |
| Allow FilesAnywhere Customer Support to Provide Technical and Administrative Support Directly to Site Users <i>(includes standard email and phone support for technical questions and password reset requests; at no additional charge)</i> | YES | |

| System Access Restrictions | Default Setting | Customer Setting |
|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------|
| IP Restrictions on Web Site <i>(only a select number of fixed IP addresses can access the Web features)</i> | No IP Restrictions | |
| IP Restrictions on Webfolder/FTP Access <i>(only a select number of fixed IP addresses can access the Webfolder or FTP features)</i> | No IP Restrictions | |

Global Security Policy

Some of the above site-level security settings can be maintained by the System Administrator from the customer organization, in the Web Admin Console, for Private Sites and Dedicated Servers. The following is a screen capture of the Global Security Policy screen:



User-Level Security Options

The System Administrator from the customer organization can use the Web Admin Console to restrict the Storage Size for users (i.e. Disk Quota for user account), or disable all Uploads to the user account (making the entire account read-only), and has the option to implement automated AutoPurge of account files (content aging without user intervention).

New User

| | |
|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Login Username: <input type="text"/> | Password: <input type="text"/> <input type="button" value="Random"/> |
| First Name: <input type="text"/> | Last Name: <input type="text"/> |
| Division: ---Select One--- | Storage Size: <input type="text" value="500"/> MB |
| Email Address: <input type="text"/> | Work Phone: <input type="text"/> |
| Cell Phone: <input type="text"/> | Home Phone: <input type="text"/> |
| Address: <input type="text"/> | |
| City: <input type="text"/> | State: <input type="text"/> |
| Zip: <input type="text"/> | Country: <input type="text"/> |
| Notes: <input type="text"/> | |
| <input type="checkbox"/> Disable Upload to Account (uploading to GroupShares still allowed) | |
| <input type="checkbox"/> Show GroupShares as Top Folder | |
| <input checked="" type="checkbox"/> Disable FileViews Feature (FileViews folder will be hidden) | |
| <input type="checkbox"/> Allow Non-Expiring Links (indefinite FileShare/Dropbox email links) | |
| <input checked="" type="checkbox"/> Automatically Purge User Files Older Than: <input type="text" value="7"/> Days | |
| <input type="checkbox"/> Remote Backup (automated transfers, backups, FTP, WebFolders) | |
| Please contact Customer Support to enable Remote Backup features. | |
| Status: <input type="text" value="Active"/> | Status Date: <input type="text" value="9/23/2005 4:11:52 PM"/> |
| Status Description: <input type="text"/> | |

MORE INFORMATION

Should you have any further questions about our data security, please don't hesitate to reply or call at the number provided below. For reasons of security, details of our internal security measures and methods are intentionally not made readily available to the public.

We can demonstrate to you the customized security measures available with our Private Site plans. Please contact us if you are interested in the multi-user Private Site.

Additional information is available from our online documentation. Please refer to this link to read more about FilesAnywhere features, frequently asked questions, and company information:

<http://www.filesanywhere.com/Help/Introduction.htm>

Live Data Center Webcam:

<http://dcwebcam01-dllstx2.theplanet.com/popup.html>



FilesAnywhere Customer Service

866.805.1991 USA Toll-free

817.835.0492 Dallas-Fort Worth, Texas

817.358.0824 Fax

FilesAnywhere.com

1001 W. Euless Blvd., Suite 206

Euless, TX 76040-5032 USA

Email Support: support@filesanywhere.com



FilesAnywhere

You've always got it.